In reply refer to: 08

September 8, 2022

VIA: **(Delivery Method)** emailaddress3

firstname lastname

address1\_line1 address1\_line2

address1\_city, govcdm\_address1statepicklist address1\_postalcode

**SUBJECT:** **Assignment of an EEO Investigator to Investigate Your Complaint of Discrimination – Case No.** **govcdm\_name, Filed** **govcdm\_dateformalcomplaintfiled**

Dear firstname lastname:

1. This is to inform you that firstname lastname of the Office of Resolution Management, Diversity & Inclusion (ORMDI) is being assigned to investigate this complaint.This letter serves to authorize the Investigator to (a) investigate the accepted claims of this complaint; (b) require all employees of the agency to cooperate with the investigation; and (c) require employees having any knowledge of the matter accepted for investigation to furnish testimony without a pledge of confidence. Pursuant to 29 C.F.R. §1614.108(c)(2), the Investigator’s authority to administer the oath is automatic during the course of this investigation.

2. The Investigator will contact you in the near future to inform you of when the investigation will begin. Should you have any questions, please contact firstname lastnameat address1\_telephone3 **XXX-XXX-XXXX** orinternalemailaddress **email**. **You are *strongly encouraged* to use email to submit your correspondence and/or documents to ORMDI.**

3. When the investigation is complete you will receive a copy of the investigation file as well as a digitized copy of the file on a CD. If you have opted for Electronic Delivery of Documents, you will receive only a CD. Should you wish to also receive a printed copy of the file, please inform the investigator in writing. The CD that you receive will be fully text searchable and can be bookmarked. It is an identical copy of the CD that is provided to EEOC should you request a Hearing. The password for the CD is **Va$eo115**.

Sincerely,

firstname lastname

District Manager

Enclosure: PA/HIPAA Notice

**Privacy Act, 5 U.S.C. 552a, and**

**Health Insurance Portability and Accountability Act (HIPAA)**

**Violation Notice**

**You are hereby being informed that the Office of Resolution Management is required to report all Privacy Act and/or HIPAA violations**.

The Privacy Act, 5 U.S.C. §552a, applies to any records about an individual which are retrieved by that individual’s name or personal identifier (such as Social Security or C-File number). The Department of Veterans Affairs maintains over eighty systems of records. ORM personnel will encounter some of these systems when performing their duties. Some examples are Patient Medical Records (24VA136); General Personnel Records (Title 38) – VA (76VA05); General Personnel Records (Title 5) (OPM/GOVT-1); and Veteran, Employee and Citizen Health Care Facility Investigation Records – VA (32VA00).

The purpose of the Privacy Act of 1974 is to balance the government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies’ collection, maintenance, use, and disclosure of personal information about them.

The Privacy Act contains a “no disclosure without consent” rule that states no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

The Privacy Act further provides for criminal penalties as follows: Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

**~~~~~~~~~~~~~~~~~~~~~~~~~**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides security standards and safeguards for individually identifiable health information. The term "individually identifiable health information" means any information, including demographic information collected from an individual, that

a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or

(c) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The "Safeguards" portion of the Act provides that each person who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards

a) to ensure the integrity and confidentiality of the information;

b) to protect against any reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information; and

c) otherwise to ensure compliance with this part by the officers and employees of such person.

The Act further provides for penalties of "wrongful disclosure of individually identifiable health information" as follows:

(a) **OFFENSE-**-A person who knowingly and in violation of this part

1) uses or causes to be used a unique health identifier;

2) obtains individually identifiable health information relating to an individual; or

3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

(b) **PENALTIES**--A person described in subsection (a) shall

1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both;

3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

**~~~~~~~~~~~~~~~~~~~~~~~~~**

**If you provide protected information belonging to other individuals (i.e., VA patients or coworkers) without their written consent during the processing of your EEO complaint, this information will be returned to the entity responsible for maintaining such records and disciplinary action may be taken against you for unauthorized use and disclosure of protected information.**